NPS Information Technology Policy/Standard

Category: 200 – Communications Network

Standard/ Policy: 202 – Wireless Network Policy

Approval: Code 05 via the Superintendent's IT Strategic Planning Taskforce

Timeline: Revision date: 11 Feb 2002
Effective date: 28 Feb 2002
Migration due date: Continuous

Definitions: A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs. The standard includes an encryption method, the Wired Equivalent Privacy algorithm (WEP).

SSID - Service Set Identifier
WECA - Wireless Ethernet Compatibility Alliance.
WiFi™ - The standard for wireless technology (IEEE 802.11).

Policy: *The policy goals are*:

- To provide guidelines that allow research and experimentation with wireless technology as it matures in ways that minimizes the possible negative impact on others.
- To limit the potential security risks that may be associated with wireless network technologies.
- To educate the NPS community about the benefits of wireless networking at NPS.
- To communicate the intent and directions with respect to the deployment of a wireless network on the NPS campus.
- To establish the NPS standards for deployment of a wireless network.

Scope:

All wireless access points that are connected by any means to the campus wired network are considered within scope of this policy and will be managed according to this policy with special attention to:

- The **security** of the NPS network will be maintained, requiring an adequate means of ensuring that only authorized users are able to access the network resources.
- The **integrity** and quality of existing wired network services will be maintained.
- **Reliability** is a concern due to possible radio interference from other wireless (or cordless) devices.
- **Suitability** refers to the deployment of a wireless network in appropriate locations for a select set of purposes; i.e., wireless is not suitable for all locations and applications and is not a strategic replacement for a wired infrastructure.

Specific policy:
As members of the NPS community deploy wireless network technology, the following steps must be taken to address the security of the campus network and promote the reliability of the wireless networks. Members of the NPS community that have already deployed wireless network technologies are required to fulfill these steps by March 20, 2002. Wireless equipment that does not meet the requirements of this policy must be disconnected from the campus network no later than 30 September 2002. All high gain antennas and amplifiers currently in use will be disconnected, replaced with wired technology, or upgraded with additional security such as IPSEC

or VPN subject to code 05 approval. A plan is to be submitted by users of high gain and/or amplification equipment for removal or upgrade no later than 28 February 2002. The use of high gain antennas and amplifiers increases the school's footprint and thus increases its vulnerability to attack. This technology should be avoided unless other alternatives are unavailable or significantly cost prohibitive.

Advance Notification: When planning to install a wireless access point, notification must be made to the NPS Network Operations Center (NOC) via a phone call to the Helpdesk (or **complete a Remedy ticket** for the planned installation), information required includes:

- The data jack ID where the access point will be connected to the campus network.
- Frequencies (or channels) to be used by the access point.
- The manufacturer and model of the access point.
- Two separate points of contact: Administrative and technical.
- The number of expected users of the access point.
- The Network Operations Center will provide an IP Address on the wireless VLAN for each access point.

All wireless access points shall be in the same VLAN for security and troubleshooting purposes. Users must fill out a **Wireless Access Point Inventory Form** via the Intranet online form.

All new access points must support the following features:

- IEEE 802.11B
- WECA WiFi™ Approved
- Non-SSID Broadcast capability
- MAC authentication
- Flash Upgrades
- 64 and 128 WEP encryption
- Radius authentication
- 802.1X
- SNMP capable for central management of flash upgrades

All new client cards must be IEEE 802.11B/WiFi™ certified and be able to support 128-bit WEP encryption for future use. Both Access Point and Client cards use the same radios. Client cards are available in PCMCIA, USB, and PCI card form. Please note that 128 WEP encryption is not part of the IEEE 802.11B or WiFi™ alliance specification.

The NOC staff will seek out the user of a specific device if it is found to be causing interference and disrupting the campus network. In these cases, the Information Technology Division (code 05) and the **Wireless Committee** reserves the right to restrict the use of all 2.4 GHz radio devices in university-owned buildings and all outdoor spaces on the NPS Campus. Cordless Phones cause the greatest problems with 802.11 networks. It is recommended when purchasing a cordless phone buy one that transmits on the 900 Mhz or 5 Ghz frequency vice 2.4 Ghz frequency to avoid collisions.

Access Coordination: ***All*** network access must be authenticated in some manner. The NPS long term direction is to require access to all NPS wireless networks be controlled through one or more of the following emerging technologies, wireless security augmentations such as Radius, 802.1x, WEP plus, and/or VPN standards. In the mean time use the following guidelines:

- Wireless installations must require registration of the Ethernet address (i.e., the media access (MAC) address), and use the MAC address filtering capabilities of the wireless access point to only allow registered addresses to use the access point.

- Users must use WEP (Wired Equivalent Privacy) keys to limit the number of people that have unencrypted access to the network. The keys must be kept as a shared secret. Members of the NPS community must inform users how to properly configure WEP. The 64-bit version of WEP should be used in the short term to support legacy systems. When funding becomes available for a campus wide implementation 128 encryption with dynamic keys will be universally installed.

Encryption: All wireless installations must turn on the Wired Equivalent Privacy (WEP) feature in an effort to protect user data. WEP should not be considered a complete protection, as it can be deciphered quickly and easily using the commonly available hacking tools. In the near future, dynamic WEP unique session key assignment will be used to provide additional security of user data as mentioned before as a wireless security augmentation. The NPS ISSM will assign and distribute a centrally managed WEP Key.

Network Name: The NOC will assign a network name, SSID code and WEP key. The SSID and WEP key will be the same for all access point to allow for campus roaming and security standardization. The SSID will be set in non-broadcast mode as security measure.

Notice of Service Activation: Departments must notify the NOC when an access point is placed in service **or** taken out of service. Notification should be made through the online Remedy system at **http://intranet.nps.navy.mil/Code05/New05/remedyldr.htm** or by phoning the help desk at extension 1046.

Large Scale Deployments: Departments with a large-scale installation of more than 50 users must arrange a meeting with the NOC Manager at x3698, to discuss additional issues that must be taken into account to maximize the potential for success.

Applications that use NetBEUI or Apple Talk to access resources will, instead, have to use IP to access those resources. For most modern applications this is not a problem, but some reconfiguration may be required.

Shared Resources: Shared resources such as printers, servers, scanners, etc. should be placed on the wired network to allow for most efficient and reliable access.

Placement of equipment: All wireless equipment must be placed in locations and set to frequencies that coordinate reasonably with campus network mechanisms. While the 802.11 standard has 12 channels only three channels do not overlap: **c**hannels 1, 6, and 11. Channels 1 and 6 will be used for common access campus wide infrastructure and channel 11 will be reserved for research. All stations need to be locked down or placed in a protected closet to prevent theft. Customized antennae to provide required coverage of surrounding areas may be needed. These adjustments are the most difficult aspect of deploying wireless base stations and should be carefully coordinated through the NOC**.** Technical design meetings are crucial and should focus on coverage and not capacity.

Personally owned wireless access points **WILL NOT** be connected to the NPS network. Users are expected to abide by the user agreement and conduct themselves in a proper fashion. If a user wishes to connect to the network using their personal system (Laptop, desktop, handheld device, etc.) they must provide the details of their system to the help desk. Details must include, at least, the following information: Manufacturer, Operating System and MAC Address.

Standard: The FCC authorizes unlicensed spectrum at the 902-928Mhz, 2.400-2483.5Ghz and 5725-5850 GHz frequency ranges. Unlicensed spectrum is also called the Industrial, Scientific, and Medical band or ISM for short. This means anyone can transmit and receive at these frequency ranges without a license as long as the devices transmits under one watt. Consumer electronic devices such as cordless phones and wireless camera will transmit at one of these frequency ranges. All

devices are required to be labeled with their frequency transmission characteristics on the device. 900 Mhz and 2.4 GHz frequencies are by far the most common. Cell phones transmit on licensed frequencies and are not limited to the 1-watt limit. The following wireless ISM frequency standards are the most common 802.11, 802.11b, 802.11A, HiperLan, HomeRF, and Bluetooth (802.15). The 802.11 specification transmits at 2.4 GHz, 802.11b standard transmits on the 2.4 GHz frequency, the 802.11a transmits on the 5 GHz frequency, HiperLan (European technology) transmits on the 5 GHz. frequency and Bluetooth (802.15) spec transmits at 2.4 GHz.

Guidelines: The campus network is a shared resource in which one individual's actions can adversely affect the network performance of others. The intent of this policy is to provide guidance and documentation on how to best use wireless technologies at the Naval Postgraduate School in the framework of the larger campus network. Failure to follow these guidelines and procedures may result in degraded network service, the loss of network connectivity and/or resources wasted to correct problems.

It is expected that general access equipment will be placed at the invitation of the management of a department, so there should be little chance of disruption of an on-going activity. However, in multi-department buildings, one department may ask to add the building to the general access network when there is a private network in place. In such cases, this policy requires that the private network be adjusted so that it does not interfere with the general access network or that it is incorporated into the general access network as part of the general infrastructure.

Transition: As technology advances, new configurations and standards will be adopted.

Technical Considerations: Other wireless technologies such as IEEE 802.11a, Home RF, Bluetooth and legacy wireless equipment exist. At this time, they will **NOT** be supported for any enterprise installation. The reason for this is as follows:

- 802.11A and HiperLan 2 despite having higher data rates do not enjoy the range of 802.11B and have not been as thoroughly tested for enterprise installations. Secondly 802.11A and HyperLan 2 function at the 5Ghz frequency and are incompatible with 802.11b equipment.
- Home RF and Bluetooth have slower data rates, shorter ranges and are incompatible with 802.11b. They transmit on the same 2.4 Ghz frequency and may cause collisions with an 802.11b network.

This is not to say that these devices will not be allowed. They will be allowed in research and test labs but users will need to go directly to the vendors for technical support. The Bluetooth focus has changed from a wireless local area network to the smaller ad hoc personal area networks. Bluetooth devices are used as cable replacement for PDAs, printers, and cell phones. Great effort is being invested by industry to ensure these devices can coexist with 802.11b equipment. As with the 802.11b devices all 802.11a, HomeRF and Hiperlan devices are required to be registered with the Network Operating Center (NOC). Bluetooth is more of a communication standard for peripheral devices and will not be required to be registered. The 802.11g standard, which expects to have products by 2003, is claming to be backwards compatible with 802.11b and enjoys similar data rates with 802.11A and HiperLan without the range limitations. If the 802.11g lives up to its claims it has the best hope of being the upgrade for an 802.11b enterprise network.

Frequency collisions: Members of the NPS community should be aware that the FCC does not license use of the frequencies used by 802.11b wireless Ethernet, and therefore other devices that use the same frequencies may disrupt wireless communications. The frequencies used by the 802.11b standard are in the unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) band. Future implementations of other 802.11 standards are planned for other unlicensed bands. Other devices that also use these unlicensed bands include but are not limited to cordless telephones, cameras, microwave ovens, cordless speakers, sprinkler control systems, and traffic light

signaling. Because 802.11 services are planned for enterprise use and support, collisions in those frequency bands need to be managed to ensure the service quality required by the users.

Equipment: Despite the existence of an 802.11b standard, campus-wide support will be enhanced by the use of a fairly uniform set of equipment. Therefore, the wireless committee strongly encourages members of the NPS community to buy wireless access points that have been tested for interoperability and feature set. A list and discussion of access point products tested will be available from the Wireless Web page. The wireless committee believes that the model of wireless Ethernet card for end-user computers is less critical, but recommends using well-established vendors. Nevertheless, 128 WEP is included on the vast majority of the equipment available today. Older equipment may be able to be upgraded via flash ROM. Often this upgrade is free and can be accomplished by a download from the manufacture's site. A list of WiFi[tm] certified products can be found on the WECA certified products page.

Rationale:

Wireless networking is not considered to be a replacement for a well-wired campus. In the near future, wired access speeds are likely to stay significantly faster than wireless technologies. As applications that require higher bandwidth become commonplace, wireless network technology may not be able to provide a suitable network connection.

Thus, wireless should be seen as an augmentation to the physical wire plant, extending the network for general-purpose network access into zones of transient use (such as common areas), and enabling applications that require the mobility offered by wireless but don't require the bandwidth or reliability of wired connections.

Due to the shared bandwidth nature of wireless, it can only support a limited number of users in a given area. Consequently, the more users, on a given frequency, the smaller the share of the bandwidth available to each user. So wireless is less appropriate in areas of high user density, especially if high bandwidth applications are a requirement. Given the limited bandwidth available per user, wireless currently works best for the relatively low bandwidth applications, such as Web browsing and e-mail.

Migration to Standard: As technology advances, new configurations and standards will be adopted.

Expectations/ Responsibilities: The end-users of wireless technology can expect to experience a significant "learning-curve" as the technology advances and the standards are modified/accepted. End-users are responsible for ensuring that the wireless environment conforms to this NPS policy.